Annual 47 C.F.R. §64.2009(e) CPNI Certification
EB Docket No. 06-36

Annual 47 C.F.R. §64.2009(e) CPNI Certification covering the prior calendar year 2018.

Date Filed: February 15, 2019

Company Name: West Telecom Services, LLC

Form 499 Filer ID: 824874

Name of signatory: Ronald Beaumont

Title of signatory: President

I, Ronald Beaumont, certify that I am an officer of West Telecom Services, LLC ("WTS"), and acting as an agent of WTS, that I have personal knowledge that WTS has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. §64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how WTS's procedures ensure that WTS is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

WTS has not taken any actions (*i.e.*, proceedings instituted or petitions filed by a company at state commissions, the court system, or at the Federal Communications Commission) against data brokers in the past year.

WTS has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

WTS represents and warrants that the above certification is consistent with 47 C.F.R. §1.17, which requires truthful and accurate statements to the Commission. WTS also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed: Ronald Beaumont

Ronald Beaumont
President
West Telecom Services, LLC

Accompanying Statement to Annual 47 C.F.R. §64.2009(e) CPNI Certification

West Telecom Services, LLC ("WTS") has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("FCC") rules pertaining to customer proprietary network information ("CPNI") set forth in sections 64.2001 – 64.2011 of the Commission's rules. This attachment summarizes those practices and procedures.

1. **Identification of CPNI.** WTS has established procedures to identify what customer information is CPNI consistent with the definition of CPNI under 47 C.F.R. § 64.2003(g) and 47 U.S.C. § 222(h)(1).

2. **Uses of CPNI Not Requiring Customer Approval.** WTS has established procedures to identify uses of CPNI that do not require customer approval under 47 C.F.R. § 64.2005 and 47 U.S.C. § 222(c)-(d). WTS may use CPNI without customer approval to (a) initiate, render, repair, maintain, bill, troubleshoot, and collect for services provided by WTS, (b) protect WTS's rights and property or to protect its subscribers or other carriers from the unlawful or fraudulent use of WTS's services, (c) provide call location information required in connection with emergency services, (d) market services formerly known as adjunct-to-basic services, (e) market WTS's services within the categories of services to which the customer already subscribes, and (f) respond to a valid request from law enforcement, a court order, or other appropriate authority.

3. **Uses of CPNI Requiring Customer Approval.** WTS has established procedures to identify uses of CPNI requiring customer approval under 47 C.F.R. § 64.2007 and how to properly obtain approval to use, disclose, or access CPNI under the Opt-Out, Opt-In, and One-Time Use notification methods under 47 C.F.R. § 64.2008.

4. **Procedures Protecting Against Disclosure of CPNI.** WTS has established procedures to protect against the disclosure of CPNI, in accordance with 47 C.F.R. § 64.2010, including without limitation: (a) authentication of customers before disclosing CPNI on customer-initiated calls, (b) prohibiting disclosure of Call Detail Information on inbound calls and providing such information only by mail to the customer's address of record, and (c) implementing procedures to provide immediate notification to customers of account changes.

5. **Record-Keeping Requirements.** WTS has established procedures on CPNI record-keeping requirements under 47 C.F.R. §§ 64.2008(a)(2), 64.2009 and 64.2010(d). The WTS CPNI Policy Administrator is required to collect and maintain records related to any (a) CPNI security breach for at least two years, (b) efforts to obtain approval to use, disclose, or access CPNI under the Opt-Out, Opt-In, and One-Time Use notification methods for at least one year, and (c) sales and marketing campaign that uses CPNI for at least one year.

6. **Reporting Requirements.** WTS has established procedures on CPNI reporting requirements under 47 C.F.R. §§ 64.2009(f) and 64.2011. WTS employees are required to immediately report (a) any unauthorized disclosure, use, or access of CPNI or breach of any database containing CPNI, and (b) any malfunction in WTS's use of the Opt-Out notification

method for obtaining customer approval to use, disclose, or access CPNI. In the event of a CPNI security breach, WTS will comply with all applicable breach notification laws.

7. Training and Disciplinary Process. WTS employees having access to, or occasion to use CPNI, are required to receive training on CPNI, which includes instruction on when they are and are not authorized to use CPNI under 47 C.F.R. § 64.2009(b). WTS also has in place an express disciplinary process to address any unauthorized use, disclosure, or access of CPNI pursuant to 47 C.F.R. § 64.2009(b).

8. Additional Safeguards. WTS has developed additional safeguards to protect CPNI, including (a) requiring its employees to verify prior opt-in or opt-out customer approval before using, disclosing, or accessing CPNI, (b) prohibiting WTS employees from providing customers with lost passwords over the telephone, (c) requiring independent contractors and joint venturers to enter into confidentiality agreements, (d) prohibiting all third parties from using CPNI for marketing purposes, (e) requiring prior approval by the CPNI Policy Administrator of all vendor contracts that will result in the disclosure of WTS customer CPNI, (f) prohibiting WTS employees from using proprietary information obtained from other carriers for purposes not intended by such carriers, (g) prohibiting WTS employees from using, disclosing, or permitting access to CPNI to identify or track customers that call competing service providers, and (h) establishing a supervisory review process for sales and marketing campaigns that use customer CPNI.